入侵事件的外部警报

以下主题介绍如何配置入侵事件的外部警报：

入侵事件的外部警报

入侵事件的外部警报通过基于配置的入侵策略和规则设置发送警报，提供关键系统监控。它支持使用多种外部通知方法发送外部警报，并独立于警报响应运行。

外部警报方法

- 简单网络管理协议 (SNMP)：按入侵策略配置，并从托管设备发送。可以为单个入侵规则启用 SNMP 警报。
- 系统日志：按入侵策略配置，并从托管设备发送。在入侵策略中启用系统日志警报会激活该策略中每条规则的警报。
- 电子邮件：在所有入侵策略中配置，并从 Secure Firewall Management Center 发送。您可以按照入侵规则启用邮件警报，并限制警报的长度和频率。

如果您配置了入侵事件抑制或阈值，系统可能不会在每次规则触发时都生成入侵事件，您可能会收到较少的警报。

注释 Secure Firewall Management Center 还使用 SNMP、电子邮件、Webhook 和系统日志警报响应来发送不同类型的外部警报。有关详细信息，请参阅使用告警响应配置外部告警。系统不使用警报响应来根据单个入侵事件发送警报。

相关主题

根据情景和频率确定入侵事件通知的优先级

入侵事件外部警报的许可证要求

要配置和使用入侵事件的外部警报，必须满足以下许可证要求：

威胁防御 许可证

您必须具有 IPS 许可证，才能为入侵事件启用外部警报功能。

配置入侵事件外部警报的要求

如果要为入侵事件配置使用 SNMP 或 系统日志 的外部警报，请确保满足以下要求：

型号支持

所有设备型号均受支持。

注释 对于运行 Snort 3 的设备，SNMP 与系统日志目标继承自访问控制策略内的日志记录设置。请注意，此配置在 Firewall Threat Defense 7.7.0 及更高版本中不可用，因为这些版本不支持 Snort 2。

支持的域

任意

用户角色

- 管理员
- 入侵管理员

配置入侵事件的 SNMP 警报

配置入侵事件的外部 SNMP 警报，以便从外部监控系统监控安全事件。启用此功能可让外部监控系统在任何已配置的入侵规则触发入侵事件时接收通知。

托管设备会在发生特定入侵事件时发送警报。

注释

- 运行 Snort 2 检测引擎的 Firewall Threat Defense 设备支持在入侵策略或入侵规则级别使用 SNMP 发出入侵事件的外部警报。在使用 Snort 3 的设备上，SNMP 陷阱目标继承自访问控制策略中的日志记录设置。
- 此配置在 Firewall Threat Defense 7.7.0 及更高版本中不可用，因为这些版本不支持 Snort 2。

过程

步骤 1 选择 **策略** > **安全策略** > **入侵** 并点击 **Snort 2 版本**。

步骤 2 在入侵策略编辑器的导航窗格中，点击**高级设置 (Advanced Settings)**。

步骤 3 启用 **SNMP警报**，然后点击 **SNMP警报**旁边的**编辑**。

页面底部出现一条消息，指明包含配置的入侵策略层。

步骤 4 选择**陷阱类型**。

步骤 5 选择 **SNMP 版本**，然后按入侵 SNMP 警报配置选项 ， 第 3 页中所述指定配置选项。

步骤 6 在导航窗格中，点击**规则**。

步骤 7 选择要为其启用 SNMP 警报的规则。然后，从**警报**下拉列表中选择**添加 SNMP 警报**。

步骤 8 要保存自上次策略确认以来在此策略中进行的更改，请选择**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果您在未提交更改的情况下离开策略编辑器，则在编辑其他策略时，未保存的更改将被丢弃。

下一步做什么

- 部署配置更改；请参阅 *Cisco Secure Firewall Management Center* 设备配置指南。

入侵 SNMP 警报配置选项

如果网络管理系统要求使用管理信息库文件 (MIB)，您可以从Secure Firewall Management Center中获取，具体位置为 `/etc/sf/DCEALERT.MIB`。

SNMP v2 选项

选项	说明
陷阱类型	警报中出现的 IP 地址所用到的陷阱类型。 如果网络管理系统正常显现 INET_IPV4 地址类型，则选择**二进制形式**选项。否则，应选择**字符串形式**。例如，HP Openview 需要选择**字符串形式**。

选项	说明
陷阱服务器 (Trap Server)	收到 SNMP 陷阱通知的服务器。可指定单一 IP 地址或主机名。
社区字符串 (Community String)	群体名称。

SNMP v3 选项

受管设备使用引擎 ID 值对 SNMPv3 警报进行编码。要解码警报，您的 SNMP 服务器需要此值，即发送设备的管理接口 IP 地址的十六进制版本，并附加“01”。

例如，如果发送 SNMP 警报的设备的管理接口 IP 地址是 172.16.1.50，则引擎 ID 值为 0xAC10013201。

选项	说明
陷阱类型	警报中出现的 IP 地址所用到的陷阱类型。 如果网络管理系统正常显现 INET_IPV4 地址类型，则选择**二进制形式**选项。否则，应选择**字符串形式**。例如，HP Openview 需要选择**字符串形式**。
陷阱服务器 (Trap Server)	收到 SNMP 陷阱通知的服务器。 可指定单一 IP 地址或主机名。
身份验证密码 (Authentication Password)	身份验证所需的密码。SNMP v3 使用消息摘要 5 (MD5) 散列函数或安全散列算法 (SHA) 散列函数进行密码加密，具体取决于配置。 一旦指定身份验证密码，身份验证即可启用。
私有密码 (Private Password)	用于保护隐私的 SNMP 密钥。SNMP v3 采用数据加密标准 (DES) 分组密码对密码进行加密。输入 SNMP v3 密码后，初始配置期间的密码会以明文显示，但以加密格式保存。 如果指定私有密码，则隐私被启用，且还必须指定身份验证密码。
用户名	SNMP 用户名。

为入侵事件配置系统日志警报

在入侵策略中配置系统日志警报，以将入侵事件发送到指定的系统日志目标。

在入侵策略中启用系统日志警报后，系统将在托管设备自身或者外部主机上向系统日志发送所有入侵事件。如果指定了外部主机，系统将从托管设备发送系统日志警报。

注释 运行 Snort 2 检测引擎的 Firewall Threat Defense 设备支持在入侵策略级别使用系统日志发出入侵事件的外部警报。对于运行 Snort 3 的设备，系统日志目标继承自访问控制策略中的日志记录设置。请注意，此配置在 Firewall Threat Defense 7.7.0 及更高版本中不可用，因为这些版本不支持 Snort 2。

过程

步骤 1 选择 **策略** > **安全策略** > **入侵** 并点击 **Snort 2 版本**。

步骤 2 在入侵策略编辑器的导航窗格中，点击**高级设置 (Advanced Settings)**。

步骤 3 启用**系统日志警报**，然后点击**系统日志警报**旁边的**编辑**。

页面底部出现一条消息，指明包含配置的入侵策略层。

系统日志警报页面添加在**高级设置**下。

步骤 4 输入您要发送系统日志警报的**日志记录主机**的 IP 地址。

如果将此字段留空，则日志主机的详细信息将从关联的访问控制策略中的日志设置中获取。

步骤 5 选择**设施**和**严重性**级别，如入侵系统日志警报的设施和严重性，第 5 页中所述。

步骤 6 要保存自上次策略确认以来在此策略中进行的更改，请选择**策略信息 (Policy Information)**，然后点击**确认更改 (Commit Changes)**。

如果您在未提交更改的情况下离开策略编辑器，则在编辑其他策略时，未保存的更改将被丢弃。

下一步做什么

- 部署配置更改；请参阅 *Cisco Secure Firewall Management Center* 设备配置指南。

入侵系统日志警报的设施和严重性

托管设备可以使用特定的设施和 **严重性**将入侵事件作为系统日志警报发送，以便日志主机可以对警报进行分类。设施指定生成警报的子系统。这些设施和 **严重性** 值不会出现在实际的系统日志消息中。

根据您的环境选择有意义的值。本地配置文件（如基于 UNIX 的日志记录主机上的 syslog.conf）可能指示将哪些设施保存到哪些日志文件中。

系统日志警报设施

设施	说明
AUTH	与安全和授权关联的消息。

设施	说明
AUTHPRIV	与安全和授权关联的访问受限的消息。在很多系统上，这些消息会转发至一个安全文件。
控制台	警报消息。
CRON	时钟后台守护程序生成的消息。
DAEMON	系统后台守护程序生成的消息。
FTP	FTP 后台守护程序生成的消息。
KERN	内核生成的消息。很多系统会在这些消息出现后将其传送至控制台打印。
LOCAL0-LOCAL7	内部进程生成的消息。
LPR	打印子系统生成的消息。
邮件	邮件系统生成的消息。
NEWS	网络新闻子系统生成的消息。
SYSLOG	系统日志后台守护程序生成的消息。
USER	用户级进程生成的消息。
UUCP	UUCP 子系统生成的消息。

系统日志警报严重性

级别	说明
EMERG	向所有用户广播的紧急状况
ALERT	应立即更正的状况
CRIT	严重的状况
ERR	错误状况
WARNING	警告消息
通知	需要注意但非错误的状况
INFO	参考性消息
DEBUG	包含调试信息的消息

配置入侵事件的邮件警报

启用入侵事件的邮件警报功能后，当入侵事件发生时，Secure Firewall Management Center 可以发送邮件通知，从而使您及时获知整个网络基础设施中的潜在安全威胁。

Before you begin

- 配置邮件主机以接收邮件警报。有关详细信息，请参阅配置邮件中继主机和通知地址。
- 确保 Secure Firewall Management Center 可以反向解析其自身的 IP 地址，因为某些邮件服务器可能会执行反向 DNS 查找来验证发件人的身份。

过程

步骤 1 选择**管理** > **警报**。

步骤 2 点击 **入侵邮件**。

步骤 3 如入侵邮件警报选项，第 7 页中所述，选择警报选项，包括要警报的入侵规则或规则组。

步骤 4 点击**保存**。

入侵邮件警报选项

配置这些入侵邮件警报选项，管理系统在入侵事件发生时发送邮件通知的方式。

开/关

启用或禁用入侵邮件警报。

注释 启用此选项后，对所有规则发送警报。选择单个规则以缩小警报范围。

发件人/收件人地址

指定邮件发件人与一个或多个收件人。使用逗号分隔多个收件人。

最大警报数和频率

设置 Secure Firewall Management Center 将按时间间隔（**频率**）发送的邮件警报最大数（**最大警报数**）。

合并警报

将具有相同源 IP 和规则 ID 的警报分组，以减少发送电子邮件的数量。

摘要输出

启用适用于文本受限设备的简要警报。简要警报包含以下内容：

- 时间戳
- 协议
- 源和目标 IP 和端口
- 消息
- 同一个源 IP 生成的入侵事件数量

示例：`2011-05-18 10:35:10 10.1.1.100 icmp 10.10.10.1:8 -> 10.2.1.3:0 snort_decoder: Unknown Datagram decoding problem! (116:108)`

如果启用**摘要输出**，还应考虑启用**组合警报**。您可能还希望降低**最大警报数**，以避免超过文本消息限制。

时区

警报时间戳的时区。

关于特定规则配置的邮件警报

选择规则以便为这些特定事件设置邮件警报。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。